UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,700	04/23/2001	Stephen Sorkin	RECOP007	4400

21912   7590   02/12/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2135	7

DATE MAILED: 02/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.		Applicant(s)
Office Action Summary	09/841,700		SORKIN ET AL.
	Examiner		**Art Unit**
	Ronald Baum		2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

    a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)   4)☐ Interview Summary (PTO-413) Paper No(s). _____.

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5)☐ Notice of Informal Patent Application (PTO-152)

3)☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5,6*.   6)☐ Other: .

DETAILED ACTION

1.   Claims 1-38 are pending for examination.

2.   Claims 1-38 are rejected.

Specification

The disclosure is objected to because of the following informalities: The attempt to

incorporate subject matter into this application by reference to US patent applications only by a

title (i.e., page 1, lines 18-21, "SYSTEM AND METHOD FOR ANALYZING LOGFILES", is

improper because reference to said documents is incomplete without more specific identification

(i.e., actual US patent applications numbers).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this
> or a foreign country, before the invention thereof by the applicant for a patent.

3.   Claims 1-38 are rejected under 35 U.S.C. 102(a) as being anticipated by NETWORK

ASSOCIATES, "Network Associates Ships Cybercop Sting", Network Associates Incorporated,

16 July 1999, ("NAI") http://www.serverwatch.com/news/print.php/1399041, entire article,

paper 5, item Q, and, STAGGS, MICHAEL "IDS:RE: cybercop sting", University of

Wollongong, Austrailia ("Staggs") via Web site

http://www.shmoo.com/mail/ids/oct99/msg00467.html , 8 October 1999, entire article, paper 5,

item J, (See MPEP 2131.01, paragraph III for multiple reference rejection criteria, where Staggs

is inherent in NAI).

4.   As per claim 1; "A method for providing security for a computer network [NAI,

paragraph 1, Staggs, paragraph 1], comprising: generating content sets for a computer associated

with the network [NAI, paragraph 2, Staggs, paragraph 1, paragraph 7, "...disinformation

files..."]; determining whether a user should be routed to the generated content sets [NAI,

paragraph 2, Staggs, paragraph 1, "...emulates...", paragraph 2, "...routes packets..."]; selecting

one of the content sets if it is determined that the user should be routed to the generated content

sets; and routing the user to the selected generated content set [NAI, paragraph 2, Staggs,

paragraph 1, "...emulates...", paragraph 2, "...routes packets..."].".

And further as per claim 35; "A system [This claim is the system of the method claim 1,

and is rejected for the same reasons provided for the claim 1 rejection above] for providing

security for a computer network, comprising: a computer configured to generate content sets for

the computer, wherein the computer is associated with the network; a plurality of network

interfaces each associated with one of the content sets; and a network device configured to

determine whether a user should be routed to the generated content sets, select one of the

generated content sets if it is determined that the user should be routed to the generated content,

and to route the user to the selected generated content set.".

Claim 36 *additionally recites* the limitations that; "The system as recited in claim 35,

wherein the network device is a firewall.". The teachings of NAI (paragraph 3, "...the

firewall...") and Staggs (paragraph 1, 3) suggest such limitations.

And further as per claim 37; "A computer program product [This claim is the embodied software on computer readable media of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for providing security for a computer network comprising a computer usable medium having machine readable code embodied therein for generating content sets for a computer associated with the network; determining whether a user should be routed to the generated content sets; selecting one of the generated content sets if it is determined that the user should be routed to the generated content sets; and routing the user to the selected generated content set.".

5.   Claim 2 *additionally recites* the limitations that; "The method as recited in claim 1, further comprising monitoring the activities of the user with respect to the computer.". The teachings of NAI (paragraph 2, "While watching...", paragraph 4, 2nd bullet "Ability to record...", paragraph 5, "...real-time intrusion monitoring...") and Staggs (paragraph 6, "...real time alarmed and logged...") suggest such limitations.

6.   Claim 3 *additionally recites* the limitations that; "The method as recited in claim 2, further comprising preventing the user from accessing files associated with said monitoring.". The teachings of NAI (paragraph 1, "...to silently monitor...", paragraph 2, "...avoid suspicion by would-be intruders..." , paragraph 3, "...a safe way to observe...") and Staggs (paragraph 6) suggest such limitations.

7.   Claim 4 *additionally recites* the limitations that; "The method as recited in claim 2, further comprising preventing the user from accessing processes associated with said monitoring.". The teachings of NAI (paragraph 1, "...to silently monitor...", paragraph 2,

"...avoid suspicion by would-be intruders...", paragraph 3, "...a safe way to observe...") and

Staggs (paragraph 6) suggest such limitations.

8.   Claim 5 *additionally recites* the limitations that; "The method as recited in claim 1,

further comprising associating each generated content set with a virtual computer.". The

teachings of NAI (paragraph 2, "...device has a real IP address...", paragraph 4, 3rd bullet

"Virtual decoy...") suggest such limitations.

9.   Claim 6 *additionally recites* the limitations that; "The method as recited in claim 5,

wherein selecting one of the content sets includes choosing a content set associated with a virtual

computer requested to be accessed by the user.". The teachings of NAI (paragraph 2, "...device

has a real IP address...", paragraph 4, 3rd bullet "Virtual decoy...") and Staggs (paragraph 7,

"...corporate competition...") suggest such limitations.

10.   Claim 7 *additionally recites* the limitations that; "The method as recited in claim 5,

further comprising associating each generated content set with its own network interface.". The

teachings of NAI (paragraph 2, "...device has a real IP address...", paragraph 4, 3rd bullet

"Virtual decoy...") and Staggs (paragraph 2, "...these virtual hosts...") suggest such limitations.

11.   Claim 8 *additionally recites* the limitations that; "The method as recited in claim 7,

further comprising concealing from the user network interfaces not associated with the selected

generated content set.". The teachings of NAI (paragraph 2, "...device has a real IP address...",

paragraph 4, 1st bullet "Detection of suspicious activity...", 3rd bullet "Virtual decoy...") and

Staggs (paragraph 2, "...these virtual hosts...") suggest such limitations.

12.   Claim 9 *additionally recites* the limitations that; "The method as recited in claim 5,

further comprising concealing from the user network connections not associated with the

selected generated content set.". The teachings of NAI (paragraph 2, "...device has a real IP address...", paragraph 4, 3rd bullet "Virtual decoy...") and Staggs (paragraph 2, "...these virtual hosts...") suggest such limitations.

13.   Claim 10 *additionally recites* the limitations that; "The method as recited in claim 9, wherein concealing network connections includes receiving a request from the user to access a network connection, checking whether that network connection is associated with the selected generated content set, and if it is not associated with the selected generated content set, providing an indication that the network connection does not exist.". The teachings of NAI (paragraph 2, "...device has a real IP address...", paragraph 4, 3rd bullet "Virtual decoy...", 4th bullet "... returns realistic packet information.", 5th bullet "... information about potential attackers...") and Staggs (paragraph 2, "...these virtual hosts...", paragraph 3, "Attacker pings10.10.10.1..." such that ping response/ non response constitutes a network connection existing / not existing.) suggest such limitations.

14.   Claim 11 *additionally recites* the limitations that; "The method as recited in claim 9, wherein concealing network connections includes receiving a request from the user to access a network connection, checking whether that network connection is associated with the selected generated content set, and if it is not associated with the selected generated content set, transforming the request into a request to access a network connection associated with the selected generated content set.". The teachings of NAI (paragraph 2, "...performs IP fragmentation reassembly...", paragraph 4, 4th bullet "... returns realistic packet information.", 5th bullet "... information about potential attackers...before they leave..") and Staggs (paragraph

2, "...these virtual hosts...", paragraph 3, "Attacker pings10.10.10.1..." such that ping response/

non response constitutes a network connection existing / not existing.) suggest such limitations.

15.   Claim 12 *additionally recites* the limitations that; "The method as recited in claim 5,

wherein the computer is running on a Unix operating system.". The teachings of NAI (paragraph

2, "...UNIX servers and routers...") suggest such limitations.

16.   Claim 13 *additionally recites* the limitations that; "The method as recited in claim 12,

wherein the computer is running on a Solaris operating system.". The teachings of NAI

(paragraph 2, "...UNIX servers and routers...") and Staggs (paragraph 1, "...Solaris 2.6

machines...", paragraph 2, "...Solaris boxes...") suggest such limitations.

17.   Claim 14 *additionally recites* the limitations that; "The method as recited in claim 1,

wherein selecting one of the content sets includes choosing a content set associated with a

service requested to be accessed by the user.". The teachings of NAI (paragraph 2, "...as finger

and FTP...") and Staggs (paragraph 3, "...a Telnet prompt...") suggest such limitations.

18.   Claim 15 *additionally recites* the limitations that; "The method as recited in claim 14,

wherein the service is telnet.". The teachings of NAI (paragraph 2, "...as finger and FTP...") and

Staggs (paragraph 3, "...a Telnet prompt...") suggest such limitations.

19.   Claim 16 *additionally recites* the limitations that; "The method as recited in claim 1,

wherein selecting one of the content sets includes choosing a content set not currently in use by

another user.". The teachings of Staggs (paragraph 3, "...a Telnet prompt...") suggest such

limitations.

20.   Claim 17 *additionally recites* the limitations that; "The method as recited in claim 1,

further comprising storing the packets sent by the user.". The teachings of NAI (paragraph 2,

"...packets destined to these hosts..." paragraph 4, 4th bullet "...log files serve...", 5th bullet

"...record suspicious activity...") and Staggs (paragraph 6, "...real time alarmed and logged...")

suggest such limitations.

21.   Claim 18 *additionally recites* the limitations that; "The method as recited in claim 1,

further comprising logging information concerning the files to which the user requests access.".

The teachings of NAI (paragraph 2, "...packets destined to these hosts..." paragraph 4, 4th bullet

"...log files serve...", 5th bullet "...record suspicious activity...") and Staggs (paragraph 4, "...a

password file? Lets grab...") suggest such limitations.

22.   Claim 19 *additionally recites* the limitations that; "The method as recited in claim 1,

further comprising preventing the user from accessing content within the computer other than the

selected generated content set.". The teachings of NAI (paragraph 4, 2nd bullet "...sacrificing any

real systems...") suggest such limitations.

23.   Claim 20 *additionally recites* the limitations that; "The method as recited in claim 1,

further comprising screening a request by the user to access a file to determine if access is

permitted.". The teachings of NAI (paragraph 4, 1st bullet "...potential attackers prying into...",

5th bullet "...information about potential attackers...") and Staggs (paragraph 6, "...real time

alarm and logged...") suggest such limitations.

24.   Claim 21 *additionally recites* the limitations that; "The method as recited in claim 20,

further comprising permitting access to a requested file if it is determined that access to the

requested file is permitted.". The teachings of NAI (paragraph 4, 1st bullet "...potential attackers

prying into...", 5th bullet "...information about potential attackers...") and Staggs (paragraph 6,

"...real time alarm and logged...") suggest such limitations.

25.   Claim 22 *additionally recites* the limitations that; "The method as recited in claim 20, further comprising providing an indication that a requested file does not exist if it is determined that access is not permitted.". The teachings of NAI (paragraph 4, 1st bullet "...to alert administrators...") suggest such limitations.

26.   Claim 23 *additionally recites* the limitations that; "The method as recited in claim 1, further comprising generating additional content subsequent to the step of generating content sets.". The teachings of Staggs (paragraph 3, "a few banners don't hurt...") suggest such limitations.

27.   Claim 24 *additionally recites* the limitations that; "The method as recited in claim 23, further comprising adding the additional content to the selected generated content set.". The teachings of Staggs (paragraph 3, "a few banners don't hurt...") suggest such limitations.

28.   Claim 25 *additionally recites* the limitations that; "The method as recited in claim 1, wherein routing the user includes using network address translation to route to the selected generated content set any user who requests to access an unauthorized service.". The teachings of Staggs (paragraph 4,5) suggest such limitations.

29.   Claim 26 *additionally recites* the limitations that; "The method as recited in claim 25, wherein the unauthorized service is telnet. The teachings of NAI (paragraph 2, "...as finger and FTP...") and Staggs (paragraph 3, "...a Telnet prompt...") suggest such limitations.

30.   Claim 27 *additionally recites* the limitations that; "The method as recited in claim 1, further comprising receiving an indication that the user is no longer connected to the computer.". The teachings of NAI (paragraph 4, 5th bullet "...before they leave.", paragraph 5 "...decoy trace-and-*track*...") suggest such limitations.

31.   Claim 28 *additionally recites* the limitations that; "The method as recited in claim 27,

further comprising determining whether to retain changes in the files of the computer that

resulted from the user's activities.". The teachings of NAI (paragraph 2 "...emulate activity of a

genuine system...", paragraph 4, 4th bullet "...return realistic packet...") suggest such

limitations.

32.   Claim 29 *additionally recites* the limitations that; "The method as recited in claim 28,

further comprising resetting the computer to restore the computer and the selected generated

content set to the condition they were in prior to the user being routed to the selected generated

content set if it is determined the changes should not be retained.". The teachings of NAI

(paragraph 2 "...emulate activity of a genuine system...", paragraph 4, 4th bullet "...return

realistic packet...") suggest such limitations.

33.   Claim 30 *additionally recites* the limitations that; "The method as recited in claim 29,

further comprising updating the selected generated content set by generating additional content

that appears to have been created during a time period during which the user was connected to

the computer.". The teachings of NAI (paragraph 2 "...emulate activity of a genuine system...",

paragraph 4, 4th bullet "...return realistic packet...") suggest such limitations.

34.   As per claim 31; "A method for providing security for a computer network [NAI,

paragraph 1, Staggs, paragraph 1], comprising: generating content sets for a file system for a first

computer associated with the network [NAI, paragraph 2, Staggs, paragraph 1, paragraph 7,

"...disinformation files..."]; creating a plurality of directories within the first computer; copying

the file system of the first computer into each of the directories [NAI, paragraph 2, Staggs,

paragraph 1, paragraph 7, "...disinformation files..."]; and routing a user who attempts to gain

unauthorized access to a second computer associated with the network to a first of the directories

in the first computer [NAI, paragraph 2, Staggs, paragraph 1, "...emulates...", paragraph 2,

"...routes packets..."].".

35.   Claim 32 *additionally recites* the limitations that; "The method as recited in claim 31,

further comprising routing a user who attempts to gain unauthorized access to a third computer

associated with the network to a second of the directories in the first computer.". The teachings

of NAI (paragraph 2) and Staggs (paragraph 2) suggest such limitations.

36.   Claim 33 *additionally recites* the limitations that; "The method as recited in claim 31,

further comprising associating at least one of the directories with a virtual computer.". The

teachings of NAI (paragraph 2) and Staggs (paragraph 2) suggest such limitations.

37.   Claim 34 *additionally recites* the limitations that; "The method as recited in claim 33,

further comprising associating each virtual computer with a network interface.". The teachings of

NAI (NAI, paragraph 1, 2) and Staggs (paragraph 1, paragraph 7, "...disinformation files...")

suggest such limitations.

38.   As per claim 38; "A computer program product for providing multiple virtual computers

on a computer [NAI, paragraph 2, Staggs, paragraph 1, paragraph 7, "...disinformation files..."]

using a Solaris operating system [NAI (paragraph 2, "...UNIX servers and routers...") and

Staggs (paragraph 1, "...Solaris 2.6 machines...", paragraph 2, "...Solaris boxes...")],

comprising a computer usable medium having machine readable code embodied therein for

generating content sets for the computer, each generated content set corresponding to a virtual

computer; allowing a user to access one of the generated content sets [NAI, paragraph 2, Staggs,

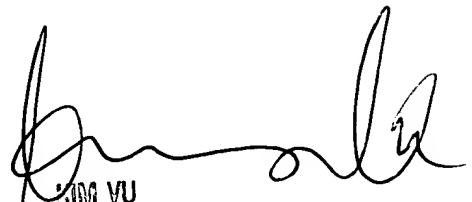paragraph 1, "...emulates...", paragraph 2, "...routes packets..."].".

Conclusion

39.   Any inquiry concerning this communication or earlier communications from examiner

should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner

can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu, can be reached at (703) 305-4393. The Fax number for the organization

where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100